UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/032,722	10/27/2001	Shigeki Kamiya	450100-03253.1	6409

20999 7590 09/01/2006

FROMMER LAWRENCE & HAUG
745 FIFTH AVENUE- 10TH FL.
NEW YORK, NY 10151

EXAMINER	
HENNING, MATTHEW T	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 09/01/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/032,722	KAMIYA ET AL.	
	Examiner	Art Unit	
	Matthew T. Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE ____ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 June 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5-8,10-13,15-18,20-23 and 25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5-8,10-13,15-18,20-23 and 25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 October 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

This action is in response to the communication filed on 6/19/2006.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 5/16/2006 has been entered.

Response to Arguments

Regarding applicant's argument that Schneier discloses splitting a message and not a key, the argument has been addressed in the advisory action dated 5/26/2006, and therefore has not been addressed further herein.

Regarding applicant's argument that the random numbers of Schneier do not guarantee uniqueness of the shares of the key, the argument has been addressed in the advisory action dated 5/26/2006, and therefore has not been addressed further herein.

Regarding applicant's argument that the cited references do not meet the limitation that the division pattern be based on the content of said digital data, the examiner does not find the argument persuasive. First, the claim does not specifically recite that the division pattern is based on the content, but rather that something is based on the content, and it is not entirely clear from the claims that the "something" that is based on the content is not the generating of the key shares. Secondly, assuming that we interpret that the division pattern is based on the content, the

cited references still meet this limitation. This is due to the only support for this limitation in the specification being on page 39 Lines 18-21, which state:

> *Additionally, **the division pattern may vary depending on the content** or may be changed periodically or irregularly during content delivery. The division pattern may also vary depending on the geographical area or the group of destinations being handled by the system.*

There is no other explanation as to the division pattern being based on the content. As such, based on the instant specification, the examiner has broadly interpreted this limitation to include division patterns which vary for different content. Schneier, teaches that when performing the splitting of the key, a random number (division pattern) is generated and used in the splitting, as is seen in Section 3.6 Step (1) of Schneier on page 70. As such, it is obvious that each time the key is split, the random number is different. Furthermore, according to Rosner, the encryption key is periodically updated and the key exchange needs to be performed again (See Rosner Col. 2 Paragraph 3). As such, when the key is updated, and the key exchange is performed again, it would be obvious that the new transmitted keys would be split according to the teachings of Schneier and therefore be accorded a new random number (division pattern). As such, the new key would be used to encrypt a new set of content, and as such the random pattern would have "varied" between the previous content and the new content. Therefore, as discussed above, the combination of Rosner and Schneier did teach the limitation of the "division pattern" being based on the content. As such, the examiner does not find the argument persuasive and has maintained the prior art combination in rejecting the claims as amended.

Claims 1-3, 5-8, 10-13, 15-18, 20-23, and 25 have been examined.

All objections and rejections not presented below have been withdrawn.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-3, 5-8, 10-13, 15-18, 20-23, and 25 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The claims recite the limitation "and based on the content of said digital data". It is unclear in the claims whether this limitation is meant to modify the division pattern, or the generating of the passkeys. As such, one of ordinary skill in the art would be unable to determine the scope of the claim. Therefore, the claims are rejected for failing to particularly point out and distinctly claim the subject matter which the applicants regard as the invention.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> *A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.*

Claims 1-3, 5-8, 10-13, 15-18, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rosner et al. (US Patent Number 6,636,968) hereinafter referred to as Rosner, and further in view of Schneier ("Applied Cryptography").

Regarding claim 1, Rosner disclosed a digital data delivery method for use in delivering digital data from all upstream system to a downstream system, said upstream system providing multipoint delivery of encrypted digital data to specific destinations, and said downstream system decrypting the delivered digital data (See Rosner Fig. 2 and Col. 4 Paragraph 3), said method comprising the steps of: encrypting digital data by said upstream system using an encryption key (See Rosner Col. 3 Lines 42-45); generating a plurality of pieces of key information on the basis of said encryption key, respective pieces of said key information being specific to each of said specific destinations (See Rosner Col. 3 Lines 48-57); delivering said respective pieces of key information to each of said specific destinations (See Rosner Col. 3 Line 57 – Col. 4 Line 7); delivering the encrypted digital data (See Rosner Col. 3 Lines 8-10); restoring said encryption key by said downstream system using said respective pieces of key information (See Rosner Col. 4 Lines 8-12); and using the restored encryption key to decrypt the encrypted digital data (See Rosner Col. 4 Lines 12-17), but Rosner failed to disclose generating the pieces of key information by dividing the encryption key by a unique division pattern, the division pattern based on the content of said digital data, or that the key information was delivered over a plurality of delivery routes which differ from routes for delivering said digital data and which are further different from each other.

Schneier teaches that key information should be delivered over a different communication channel than the data encrypted using the key information (See Schneier Col.

Page 176 Lines 34-37). Schneier further teaches that keys should be split and each part should be delivered over a separate channel (See Schneier Page 177 Paragraph 1). Schneier further teaches that the key should be split using random numbers, which would be unique for each splitting (See Schneier Pages 70-71 Section 3.6 Secret Splitting).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schneier in the partial key delivery system of Rosner by splitting and delivering the partial keys and group key used to reconstruct the decryption key over different channels and further over a different channel than the encrypted content. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the key from being illicitly reconstructed as well as to protect the encrypted content from being illicitly decrypted. In this combination, it would be obvious that when the key is updated, the key splitting would be repeated and a new random number would be generated for the splitting. Therefore, it would be obvious that in this combination, the division pattern would vary for the content that it was associated with, and as such the division pattern would be "based" on the content.

Claim 2 is rejected for the same reasons as claim 1 above and further because the passkeys of claim 2 are equivalent to the pieces of key information of claim 1 above.

Regarding claim 3, the combination of Rosner and Schneier disclosed a digital data delivery method for use in delivering digital data from an upstream system to a downstream system, said upstream system providing multipoint delivery of encrypted digital data to specific destinations, and said downstream system decrypting the delivered digital data (See Rosner Fig. 2 and Col. 4 Paragraph 3), said method comprising the steps of: encrypting digital data by said

upstream system using an encryption key (See Rosner Col. 3 Lines 42-45); generating on the basis of said encryption key, a set of passkeys by dividing said encryption key by a division pattern unique to each of said specific destinations and based on the content of said digital data (See the rejection of claim 1 above); generating a plurality of partial keys based on a portion of the passkeys in said set or a portion of passkey information from which said passkeys may be reproduced (See Rosner Col. 3 Lines 48-57 especially elements 225-227); delivering either said plurality of partial keys or partial key information, from which said partial keys may be reproduced (See Rosner Col. 3 Lines 57-60), and delivering the remaining passkeys not used to generate said partial keys or the remaining passkey information (See Rosner Fig. 2 which clearly depicts element 212a being transmitted from the source to the destination devices and Fig. 4 further confirms this), to each of said specific destinations over a plurality of delivery routes which differ from routes for delivering said digital data and which are further different from each other (See the rejection of claim 1 above); delivering the encrypted digital data (See Rosner Col. 3 Lines 8-10); restoring said encryption key by using said downstream system using either said plurality of partial keys or said partial key information and using either said remaining passkeys or said remaining passkey information delivered over said plurality of delivery routes (See Rosner Col. 4 Lines 8-12); and using the restored encryption key to decrypt the encrypted digital data (See Rosner Col. 4 Lines 12-17).

Regarding claim 5, the combination of Rosner and Schneier disclosed a digital data delivery method for use in delivering digital data from an upstream system to a downstream system, said upstream system providing multipoint delivery of encrypted digital data to specific destinations, and said downstream system decrypting the delivered digital data (See Rosner Fig.

2 and Col. 4 Paragraph 3), said method comprising the steps of: encrypting digital data by said upstream system using a first encryption key (See Rosner Col. 3 Lines 42-45); generating a second encryption key specific to each of said specific destinations and/or to said digital data (See Rosner Col. 6 Lines 23-25); using said second encryption key to encrypt either said first encryption key or first encryption key information from which said first encryption key may be reproduced (See Rosner Col. 4 Lines 55-59 Element 212a and Fig. 3 Element 'X'); generating, on the basis of said second encryption key, a set of passkeys (See Rosner Col. 4 Lines 55-59 Elements 225-228) by dividing said encryption key by a division pattern unique to each of said specific destinations and based on the content of said digital data (See the rejection of claim 1 above); delivering either said encrypted first encryption key or said encrypted first encryption key information and delivering either said set of passkeys or passkey information, from which said set of passkeys may be reproduced (See Rosner Col. 3 Lines 57-67), to each of said specific destinations over a plurality of delivery routes which differ from routes for delivering said digital data and which are further different from each other (See the rejection of claim 1 above); delivering the encrypted digital data (See Rosner Col. 3 Lines 8-10); restoring said second encryption key by using either said set of passkeys or said passkey information delivered over said plurality of delivery routes so as to decrypt either said first encryption key or said first encryption key information and thereby restore said first encryption key (See Rosner Col. 4 Lines 8-12); and decrypting the encrypted digital data by use of the restored first encryption key (See Rosner Col. 4 Lines 12-17).

Claims 6, 11, and 16 are rejected for the same reasons as claim 1 above and further because Rosner disclosed the upstream system (See Rosner Fig. 2 Element 210).

Claims 7, 12, and 17, are rejected for the same reasons as claim 2 above and further because Rosner disclosed the upstream system (See Rosner Fig. 2 Element 210).

Claims 8, 13, and 18, are rejected for the same reasons as claim 3 above and further because Rosner disclosed the upstream system (See Rosner Fig. 2 Element 210).

Claims 10, 15, and 20, are rejected for the same reasons as claim 5 above and further because Rosner disclosed the upstream system (See Rosner Fig. 2 Element 210).

Claims 21-23 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Rosner and Schneier as applied to claims 1-5 above, and further in view of Schneier.

The combination of Rosner and Schneier disclosed a system and method for communicating encrypted data using key reconstruction at the receiver (See the rejections of claims 1-5 above), but failed to disclose software for implementing the method.

Schneier teaches that any encryption algorithm can be implemented in software (See Schneier Page 225 Lines 25-38).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schneier in the encryption system of Rosner and Schneier by providing software to implement the encryption method. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide flexibility and portability, ease of use, and ease of upgrade to the encryption system.

Conclusion

Claims 1-3, 5-8, 10-13, 15-18, 20-23, and 25 have been rejected.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

CHRISTOPHER REVAK
PRIMARY EXAMINER

8/31/06

Matthew Henning
Assistant Examiner
Art Unit 2131
8/30/2006